FortiOS Certificate Management

A step-by-step guide on managing certificates in FortiOS

FortiOS can provide the security via x.509 certificates, and this functionality can be leveraged for SSL inspection, IPSec or SSL VPN. The following guide is designed to help anyone from the neophyte to the PKI guru install the certificates used in FortiOS. Follow these steps and in a short amount of time you will have your own certificate installed.

Use the Table of Contents below to quickly locate and access the tutorial of your choice.

Table of Contents

FortiOS Certificate Interface

1. First you will need to login to your FortiGate/FortiOS and go to **System** > **Certificates**.
2. Under certificates, click the "**Local Certificates**" link.

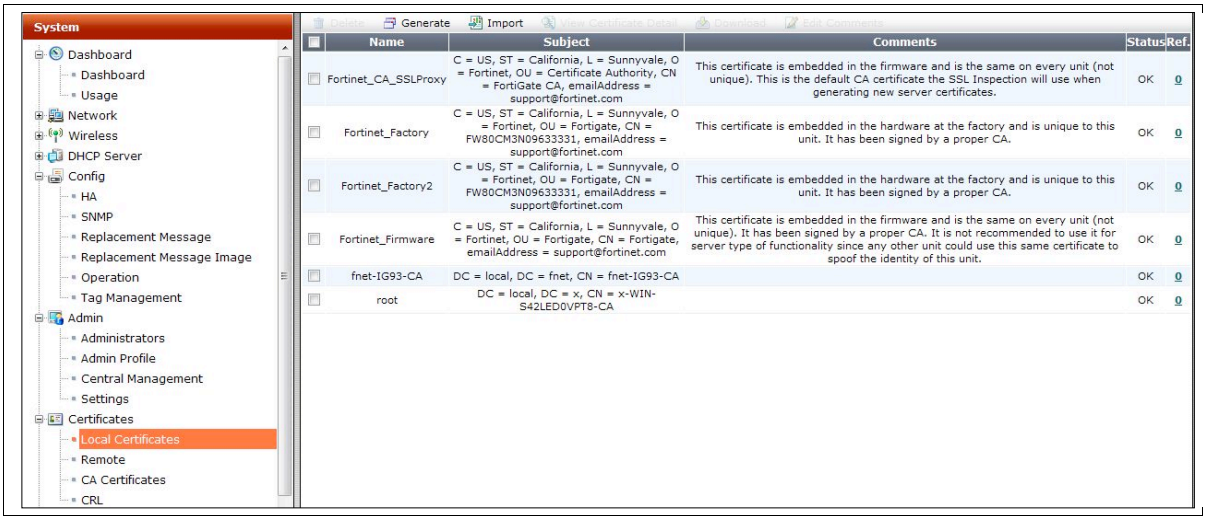


Fig 1.1

3. Here you have the option to generate or import a certificate.

Generating a Certificate in FortiOS

1. From **System** > **Certificates** > **Local Certificates**, click the "**Generate**" button to get the following screen:

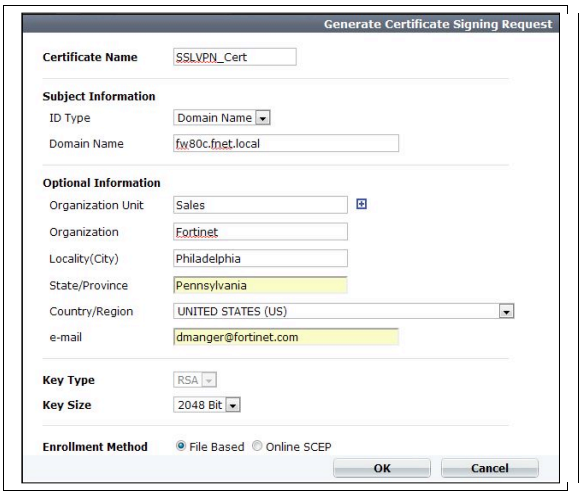


Fig 2.1

2. Enter the following information in the specified fields:

Certificate Name: This is the name of the certificate as it appears under "**Local Certificates**".

Subject Information: Here you will specify an IP, Domain Name (FQDN) or email address as the ID Type. For the purposes of this guide, I have used "Domain Name" since this will be an SSL certificate.

Note: If you wish to use a wildcard certificate, simply enter the wildcard domain in the "Domain Name" field (e.g. *. fortinet.com).

Optional Information: Although it is stated as optional, I recommend entering the information for each of the fields under this heading. Additionally, if you are generating a certificate signing request (CSR) for a third-party certificate authority (CA), you will need to insure that these values reflect those listed for your company/organization at said certificate authority. If you are generating a certificate for a Microsoft CA, you will need to check with the administrator regarding these values.

Organizational Unit: This is the name of the organizational unit under which the certificate will be issued. I have used "Sales" for my example since that is the organizational unit in which I reside.

Organization: This will be the overall name of the organization. I used "Fortinet" in my example as I work for Fortinet.

Locality: This is simply the name of the city where the SSL certificate will be located.

State/Province: For this field, it is important to note that some issuers will reject a CSR that has an abbreviated state/province. It is a best practice to always use the full name of the state/province when filling out this form.

Country: Simply select your country from the dropdown list.

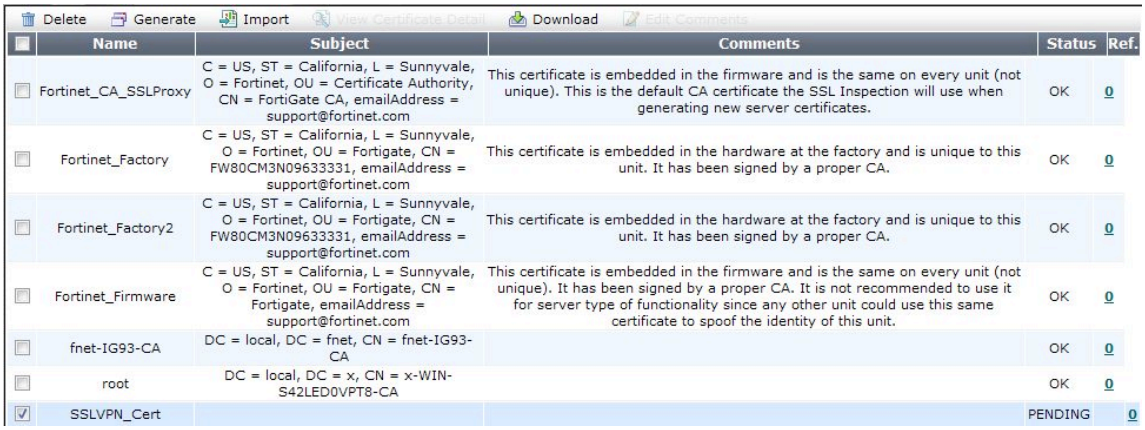
E-mail: The email address of the technical contact for the SSL certificate that is being requested.

Key Type: RSA is the base selection for this field and the only supported algorithm.

Key Size: You have a choice between 1024, 1536 and 2048 for bit-size/strength. I recommend using 2048 so long as your CA can issue certificates of that size.

Enrollment Method: Unless you or your organization has a current methodology for enrolling certificates using SCEP (Secure Certificate Enrollment Protocol), I would recommend using the default, File-Based option. This will generate a csr that can be sent to your CA for the certificate enrollment.

Once these fields are filled out, click "OK". This will take you back to the "Local Certificates" landing page where you can see your request.



	Name	Subject	Comments	Status	Ref.
☐	Fortinet_CA_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com	This certificate is embedded in the firmware and is the same on every unit (not unique). This is the default CA certificate the SSL Inspection will use when generating new server certificates.	OK	0
☐	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = FW80CM3N09633331, emailAddress = support@fortinet.com	This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.	OK	0
☐	Fortinet_Factory2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = FW80CM3N09633331, emailAddress = support@fortinet.com	This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.	OK	0
☐	Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com	This certificate is embedded in the firmware and is the same on every unit (not unique). It has been signed by a proper CA. It is not recommended to use it for server type of functionality since any other unit could use this same certificate to spoof the identity of this unit.	OK	0
☐	fnet-IG93-CA	DC = local, DC = fnet, CN = fnet-IG93-CA		OK	0
☐	root	DC = local, DC = x, CN = x-WIN-S42LED0VPT8-CA		OK	0
☑	SSLVPN_Cert			PENDING	0

Fig 2.2

3. In the latter image, you can now see that there is a "**Download**" link available for the CSR you just generated. Click the download link and save the file to your file system.
4. The resultant file (SSLVPN_Cert.cer) will have content similar to the following:

-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwgZUxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJQQTEVMBMGA1UE
BxMMcGhpbGFkZWxwaGlhMREwDwYDVQQKEwhGb3J0aW5ldDEOMAwGA1UECxMFU2Fs
ZXMxGjAYBgNVBAMTEWZ3ODBjbS5mbmV0LmxvY2FsMSMwIQYJKoZIhvcNAQkBFhRk
bWFuZ2VyQGZvcnRpbmV0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAMbG+JwLzl/o/kRf7PfQtSJg/r85JvaWLso56kfvRsRP0UVk861tJXoQuAvp
EaADYilACtTTMnNNZjkhhF9T//DFljKrV1XPyF8LPSt0P/BBsQSPq7RjlhQdHs3R
UvhCQt3yLiNYAmZ17zqsOyMNstiW0pNpq/4BrWtBDdjdKyFGePjg98Ms6RwGPNnQ
teBaulBpzdBMUO/NF1+A2cRvdGevBNandsvW3zEOCgyO1dhvlttapNefe972Ny8/
Lcqv/f/LWpJB8ZUhGRYp01m74xTHStNfSdZjFryC6K41Xvv5oaOHX1ObPxY3iGSV
m7B6on26E9NNX9/5ZDjuTquXhgECAwEAAaATMBEGA1UdEzEKEwhDQTpGQUxTRTAN
BgkqhkiG9w0BAQUFAAOCAQEAsBWD7ZiWsms5wUITlKG9EKl9l0E7vj6rphmNjyJX
nwHPTAOr/MoT31tPC6w4n59QhkSYWjmS+9BEYUSItUvuYh/e4+w14eFwdAB/UgE0
35g+vX2Z3nHMHYlD++r7squ0TUBcca6bMGPbw2Epmg8LELv64ClyRku475JlJ/Xd
rXWJugRnXE3p1uziQfimJ16/FkhsrFqWMUk0jl7zmTQG0y4WhqL1dFnZXx9LtC50
v4DHz8HakuHJxdaKHewe+oKcYhjHG6w0Nn9Bw06L6jCEAXVkRIqHOZJuhNCSaj2j
djlSEm4G7NEPpG0xhqCJHoarqmaenSLS0H1vHzl5Slp+Hg==
-----END CERTIFICATE REQUEST-----

5. Send this file either to your local certificate administrator or your third-party certificate authority for processing. Once you get the issued certificate, you can import it by clicking the "**Import**" link after selecting the certificate request you made (see Fig 2.2).

Note – SAN/UCC Certificates: When sending this file to the certificate administrator for issuance, be certain to specify the additional domains that will be listed under subjectAltName in the certificate. For example, if the certificate is being issued from Microsoft Certificate Services, the administrator will need to specify the following additional attribute for the certificate:

```
SAN:dns="111.fnet.int"&dns="test.domain.local"&dns="fg1.domain.com"
```

This will result in the Subject Alternative Name of the issued certificate containing the additional domains listed in the attribute string above.

6. From the "**Import Certificate**" page, select the certificate type (in this instance, it is of type "**Local Certificate**") and then click the "**Choose File**" button for the Certificate file. Once you have selected the appropriate certificate file, click the "**OK**" button.

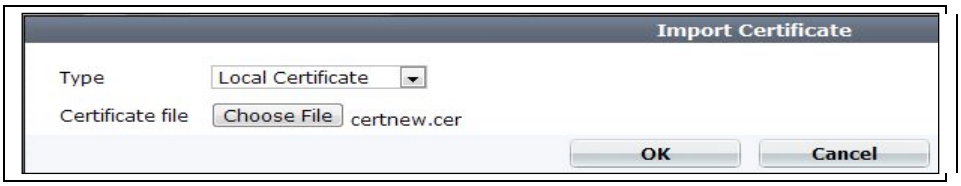


Fig 2.3

7. At this point, you should see the following message on the screen:

"Upload Certificate successfully. Return"

Now you can click the "**Return**" link and see your fully imported certificate under "**Local Certificates**". If you experience any issues with the import process, please contact your representative Sales or Support Engineer.

Generating a Certificate using OpenSSL

This section will cover the generation of a certificate using OpenSSL. In order to successfully run the following steps, you will need to download and install OpenSSL from the following URL:

Windows: http://www.slproweb.com/products/Win32OpenSSL.html
Linux/Unix: http://www.openssl.org/source/
Mac OS X: OpenSSL is preinstalled

Generating a CA certificate/private key pair:

1. Click **Start** > **Run** and enter "`cmd`" into the Open field. Click "**OK**".

2. Path to the OpenSSL bin directory using the following command:
   ```
   cd C:\OpenSSL-Win32\bin
   ```

3. From the OpenSSL bin directory, type the following command to generate a CA certificate/private key pair:
   ```
   openssl genrsa -des3 -out fgcaprivkey.key 2048
   ```

   This command will generate a private key for the CA certificate you will create in the next step. This key will leverage the RSA key algorithm, Triple Des (des3) encryption and a 2048-bit key size. This

command will require a PEM passphrase to be created for the private key. This password will be used when the private key is leveraged.

The following command will create the CA certificate using the private key that was created in the previous step:

```
openssl req -new -x509 -days 3650 -extensions v3_ca -key fgcaprivkey.key -out fgca.crt
```

This command requests a new, x.509 CA certificate that has a v3 CA extension. In addition, the command also breaks out the private key and CA certificate into two files: `fgcaprivkey.key` and `fgca.crt`.

The command will ask for the following details to be entered when creating the CA and private key files:

PEM Pass Phrase: This is the password that is required in order for you to leverage the private key of the CA. This will be needed when you import the CA into FortiOS in section, “Importing The Extracted CA Certificate and Private Key”.

Country Name: This will be the two-letter abbreviation of the country where the CA will reside.

State or Province Name: This is the full name of the state or province where the CA will reside.

Organization Name: This is the name of the overall organization under which the CA will run.

Organizational Unit: This is the name of the organizational unit under which the certificate will be issued. I have used “Sales” for my example since that is the organizational unit in which I reside.

Common Name: This is the fully qualified domain name (FQDN) of the CA certificate.

Email Address: This should be the email address of the main CA administrator/technical contact or group alias.

See the following screen shot for an example of a completed command:

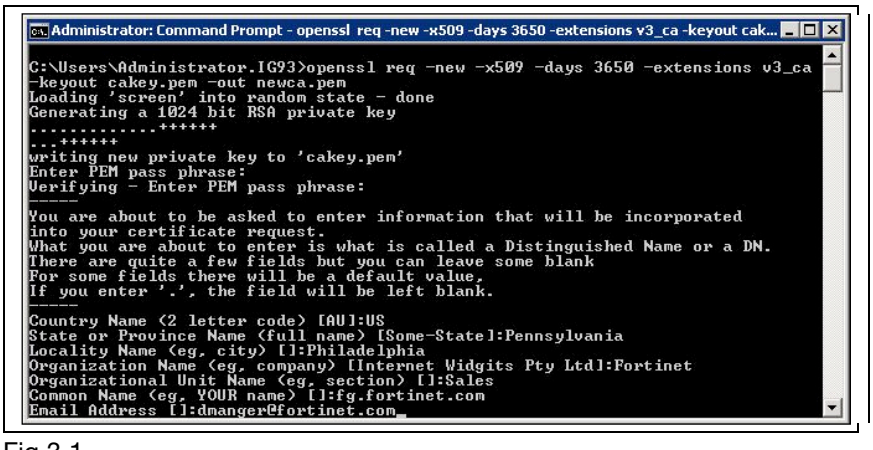


Fig 3.1

Generating a CA signed SSL Certificate

1. Click **Start** > **Run** and enter "cmd" into the Open field. Click "**OK**".

2. Path to the OpenSSL bin directory using the following command:
   `cd C:\OpenSSL-Win32\bin`

3. From the OpenSSL bin directory, type the following commands to generate the SSL certificate private key:
   `openssl  genrsa -des3 -out fgssl.key 2048`

   This command will generate a private key using the RSA algorithm (genrsa), Triple Des encryption (des3) and a 2048-bit key size. You will be required to create a password for this private key (Fig 3.1)

4. Use the next command to create a certificate signing request (CSR) for the SSL certificate:
   `openssl req -new -key fgssl.key -out fgssl.csr`

   This command will create a .csr (fgssl.csr) for the SSL certificate using the private key file created in the previous step. This command will require that you enter the PEM passphrase you created in the previous step, as well.

   You will need to fill out the same fields as those mentioned in Step 3 from the "Generating a CA certificate/private key pair" section.

   You will be asked to enter "extra" attribute information pertaining to a challenge password and optional company name. You can leave these blank.

   Note: To generate a wildcard SSL certificate, be sure to enter the wildcard domain in the "Common Name" field in the aforementioned section. An example is as follows:

   Common Name (eg, YOUR name): *.fortinet.com

5. Using the .csr that was created in the previous step, you can now create the SSL certificate using the CA certificate that was created in the section, "Generating a CA certificate/private key pair".

   ```
   openssl x509 -req -days 365 -in fgssl.csr -CA fgca.crt -CAkey
   fgcaprivkey.key -set_serial 01 -out fgssl.crt
   ```

   This command will create an x.509 SSL certificate that has been signed/issued by the CA certificate that was created prior. It has a validity period of one year and a serial number of "`01`". This certificate can now be imported into FortiOS using the method listed in the "Importing The Extracted CA Certificate and Private Key" section below.

Generating a SAN/UCC SSL Certificate

On the server where OpenSSL is installed, insure that the configuration file has the following settings enabled/uncommented:

```
copy_extensions = copy

[req]
x509_extensions   = v3_ca

[ v3_req ]
basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names



[alt_names]

DNS.1 = domain.test.local

DNS.2 = domain.test.net

DNS.3 = test.internal.local
```

Note: For [alt_names], enter the domain names specific to your organization.

1. Save the configuration changes and run the following commands:

   ```
   openssl  genrsa –des3 –out ucc.key 2048
   openssl req –new –key ucc.key –out ucc.csr
   ```

   The latter command will generate the certificate signing request (.csr). Note that when prompted for the Common Name of the certificate; enter the primary domain name for the FortiGate device. This domain name needs to be different than those specified under [alt_names] in the configuration file.

2. To create the SAN/UCC certificate, type the following command:

   ```
   openssl ca -policy policy_anything -cert cacert.crt -keyfile
   privatekey.key -in ucc1.csr -out ucc1.crt -outdir <outputDirectory>
   ```

   This command will leverage the default policy of the OpenSSL configuration to insure that the [alt_names] (subjectAltName) will be populated for the issued certificate.

3. Check that the subjectAltName values have been added to the issued certificate:

```
openssl x509 –in ucc.crt –text –noout
```

The output should contain the following information:

```
 X509v3 Subject Alternative Name:
DNS:111, DNS:111c.111c.111c, DNS:111.fnet.int
```

4. Import the SAN/UCC certificate using the steps from “Importing The Extracted Certificate and Private Key Into FortiOS”.

Generating a self-signed SSL Certificate

1. Click **Start** > **Run** and enter “`cmd`” into the Open field. Click “**OK**”.
2. Path to the OpenSSL bin directory using the following command:

   ```
   cd C:\OpenSSL-Win32\bin
   ```

3. From the OpenSSL bin directory, type the following commands to generate a self-signed SSL certificate:

   ```
   openssl  genrsa –des3 –out fgssl.key 2048
   openssl req –new –key fgssl.key –out fgssl.csr
   openssl x509 –req –days 365 –in fgssl.csr –signkey fgssl.key –out
   fgssl.crt
   ```

   Once completed, you can now import the self-signed SSL certificate into FortiOS using the steps outlined in the “Importing The Extracted CA Certificate and Private Key” section below.

Importing a Certificate into FortiOS

This section will take you through the steps of importing a certificate/private key pair into FortiOS. The import of a certificate into FortiOS will usually coincide with the need to implement a deep inspection of the HTTP protocol. For more information about the inspection of HTTPS or the proxy thereof, please refer to the FortiOS Administration Guide.

First, you will need to determine what type of certificate you would like to import. If it is a certificate for HTTPS proxy/inspection, you will need to import either your root CA or an intermediate CA. If it is simply for SSL, you will need to import the SSL certificate and private key pair. For the purposes of this document, I will be covering the import of a CA certificate into FortiOS for HTTPS proxy/inspection. The import of an SSL certificate will be the same process.

Note: The Microsoft CA will be the main point of reference in this section. If you have another CA from another vendor, the process should be similar to that which follows. Additionally, it is required that you

import the CA certificate and private key into FortiOS in order for HTTPS proxy/inspection to function properly.

There are two main ways of exporting a CA certificate/private key pair from the Microsoft Certificate authority:

Backup the CA certificate/private key pair:

1. From your CA authority server, click Start > Programs > Administrative Tools >Certificate Authority. This will open the following screen:

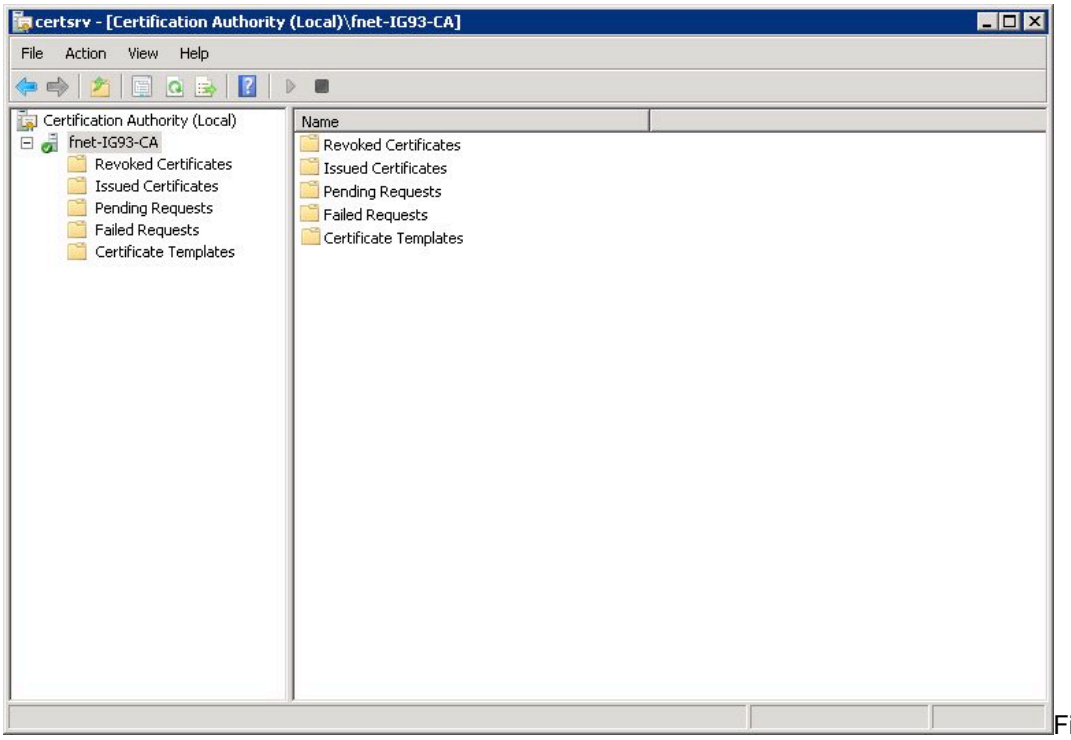


Fig 4.1

2. Right-click on the CA name (fnet-IG93-CA – Fig 4.1) and select All Tasks > Back Up CA.

3. This will start the Certificate Authority Backup Wizard.

Fig 4.2

4. Click "**Next**", then select "**Private key and CA certificate**". Provide an empty directory to where the CA will be backed up and then click "**Next**".

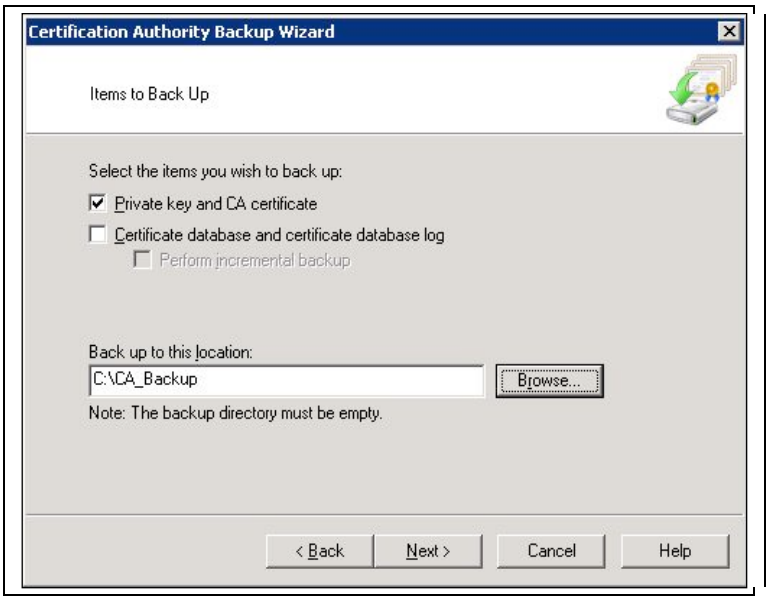
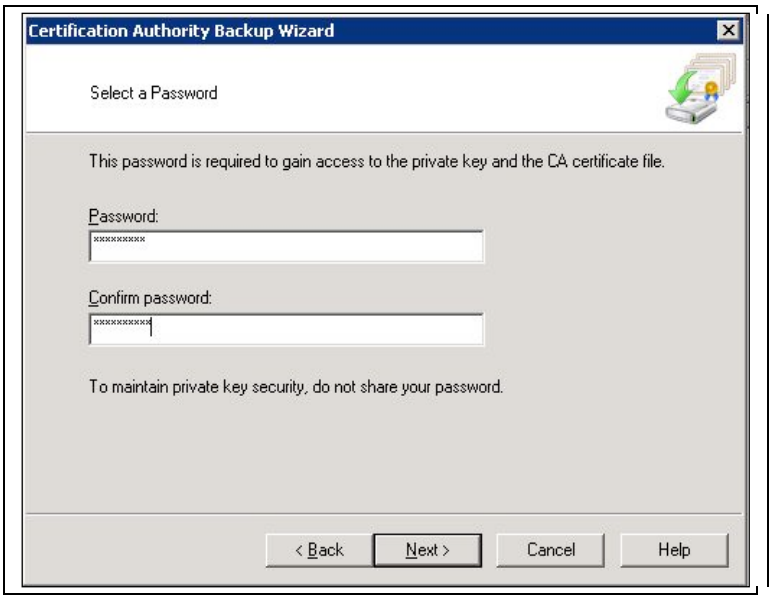


Fig 4.3

5. Enter the password that that will be required to gain access to the CA certificate and private key pair and click "**Next**".



4.4

6. You will be presented with the following screen where you can then click "**Finish**" to complete the back up process.

Fig 4.5

7. Make note of the location of the backed up CA certificate as it will be used later in this document.

Export the CA certificate/private key pair:

1. From the Certificate Authority server, click **Start** > **Run**. Type "`mmc`" into the field and click "**OK**".

2. From the console window, click **File** > **Add/Remove Snap-in**. This will open the following window:

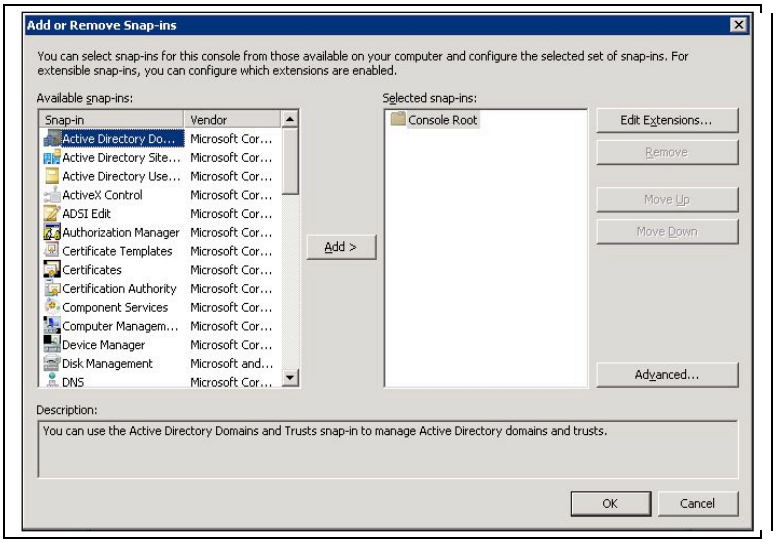


Fig 5.1

3. Select "**Certificates**" from the "**Available snap-ins**" group and add it to the "**Selected snap-ins**" group. This action will open a new window that will ask you which certificates you would like to have managed. Select "**Computer account**" as shown in the image below:

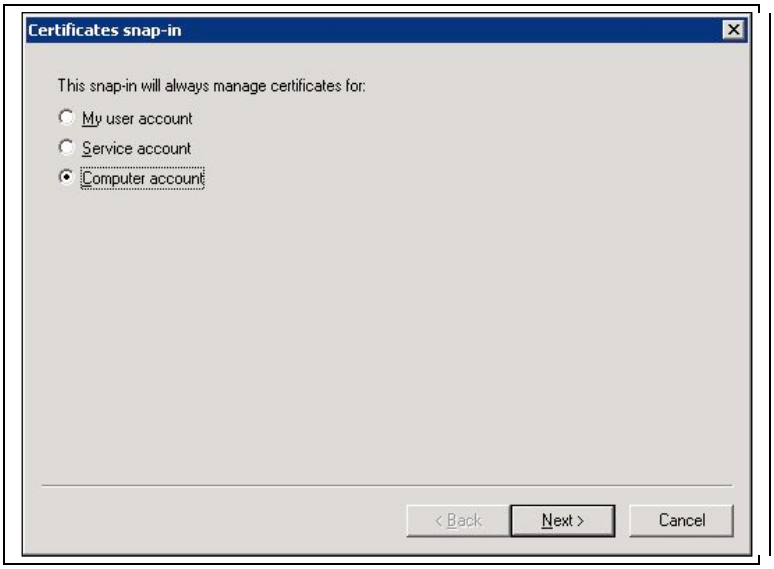


Fig 5.2

4. When you click next, another window will appear asking you to select the local computer or another computer where the certificates will reside. Maintain the selection for "**Local computer**" and click "**Finish**". Once the window closes, you will be taken back to the original window from step 3 (Fig 5.1). Click "**OK**", which will take you back to the console window.

5. From the console window, go to **Console Root** > **Certificates** > **Trusted Root Certification Authorities** > **Certificates**, as shown below:

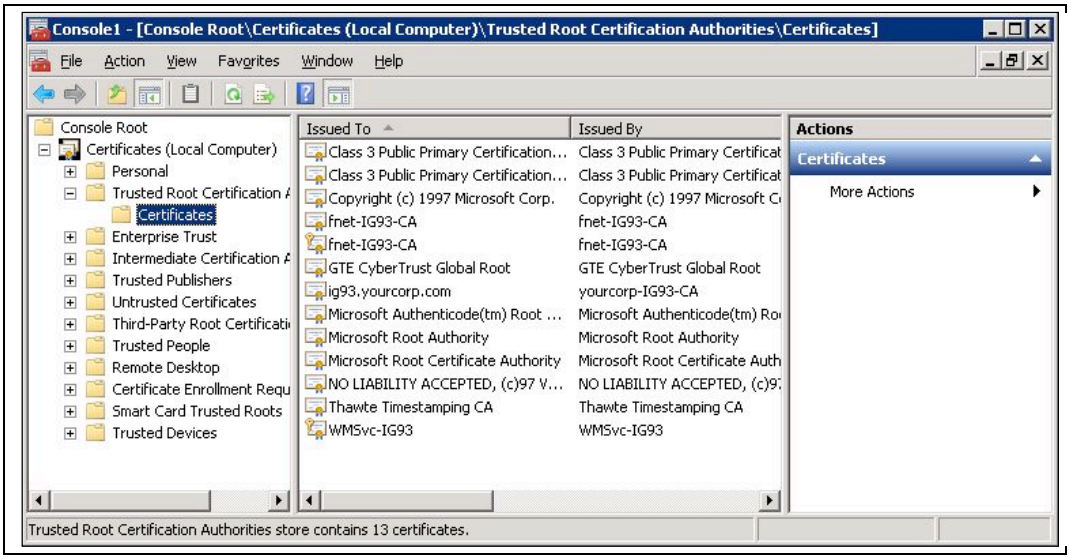


Fig 5.3

6. Right-click the CA certificate that you would like to export and select **All Tasks** > **Export**. This will open the **Certificate Export Wizard**.

Fig 5.4

7. Click "**Next**" and select the option, "**Yes, export the private key**".

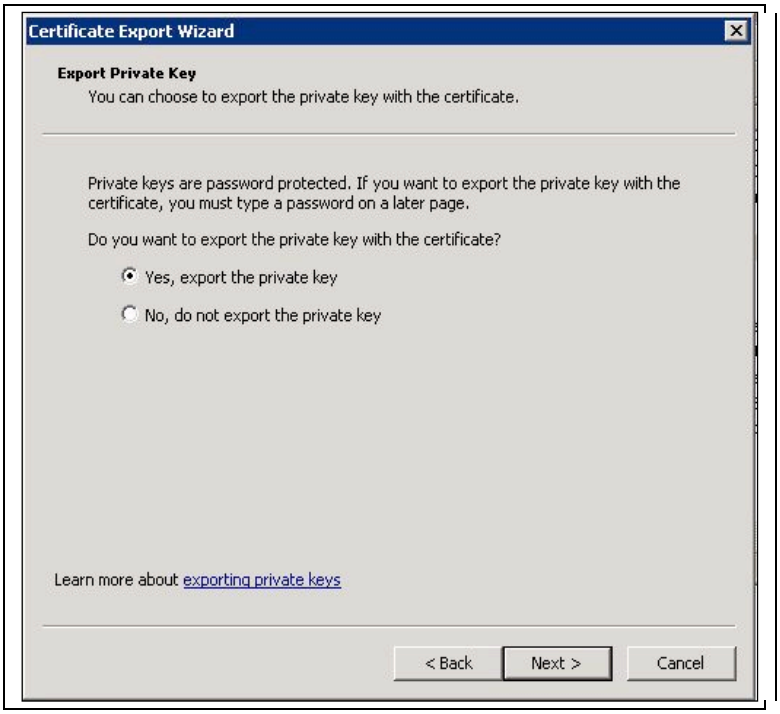


Fig 5.5

8. Click “**Next**” and insure that “**Personal Information Exchange – PKCS #12 (.PFX)**” is selected. Select any additional options per your desires and click “**Next**”.

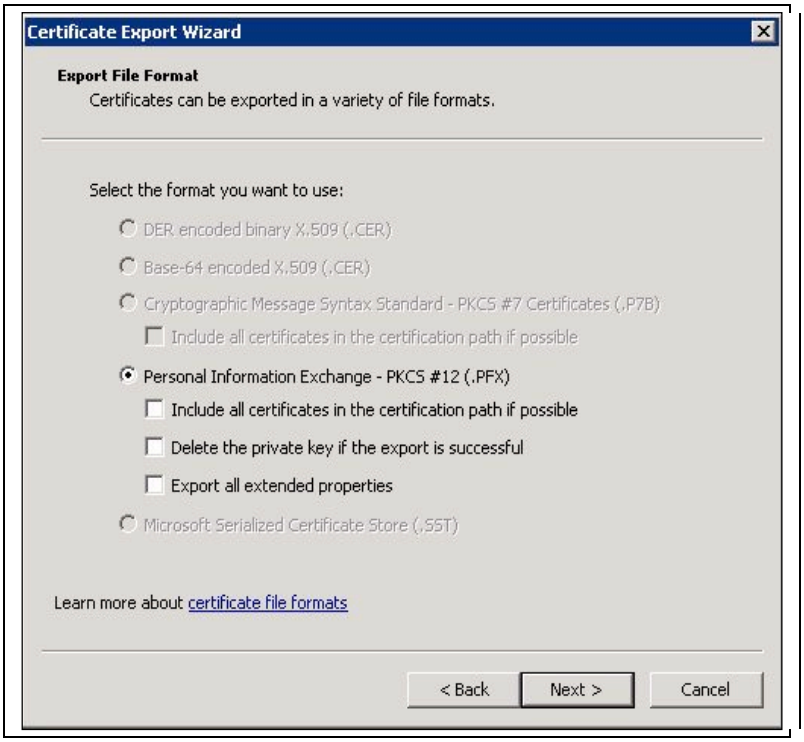


Fig 5.6

9. Enter the password that that will be required to gain access to the CA certificate and private key pair

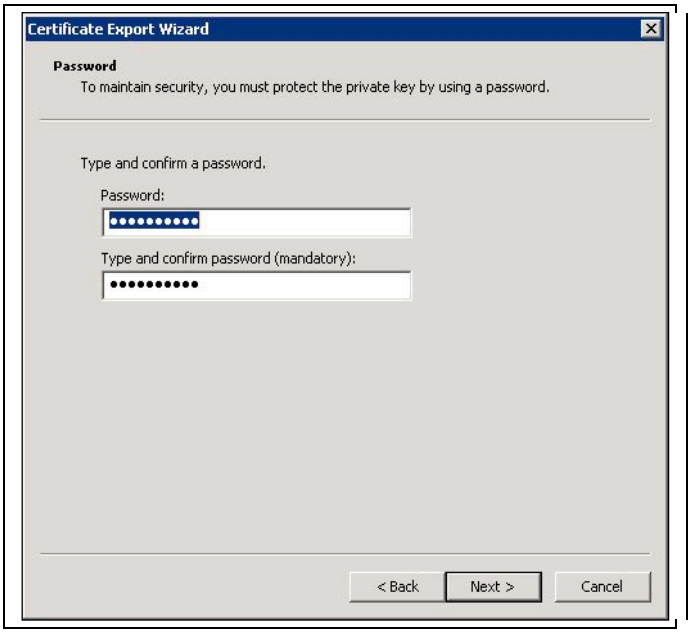


Fig 5.7

10. Enter the path to where the certificate will be exported. Click "**Next**" and then "**Finish**" on the next screen. You have successfully exported your CA certificate/private key pair.

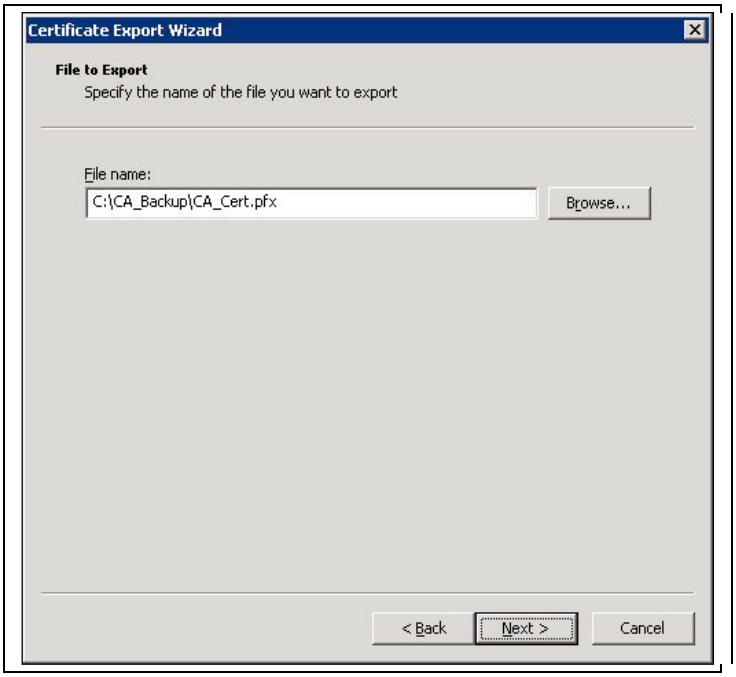


Fig 5.8

Extracting the CA Certificate Private Key

This section details how you will extract the private key from the CA Certificate/private key pair you exported using one of the latter two methods.

Additionally, copy the exported CA certificate/private key file to your file system if you are not using the CA server for OpenSSL.

Use the following steps to extract the CA certificate private key:

4. Click **Start** > **Run** and enter "`cmd`" into the Open field. Click "**OK**".

5. Path to the OpenSSL bin directory using the following command:

   ```
   cd C:\OpenSSL-Win32\bin
   ```

6. From the OpenSSL bin directory, type the following command to extract the private key from the CA certificate/private key pair:

   ```
   openssl pkcs12 -in <exportedCAcertificate>.pfx -nocerts -out
   C:\privatekey.key
   ```

Note: The <exportedCAcertificate> notation above indicates that you should substitute the file name of the exported CA certificate. The command referenced shows a pfx extension, but p12 can be used, as well. Also, when you hit enter, you will be prompted to provide the password that you set when exporting/backing up the CA certificate.

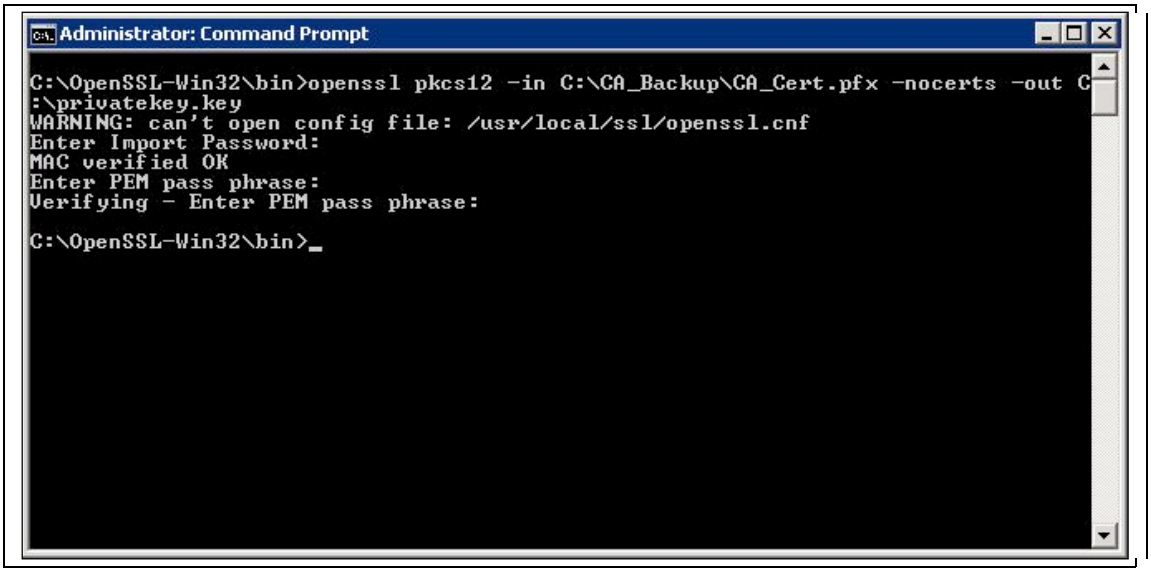


Fig 6.1

7. Using the same command line session, type the following command to extract the CA certificate without the private key:

```
openssl pkcs12 -in <exportedCAcertificate.pfx -clcerts -nokeys -out
C:\cacert.crt
```

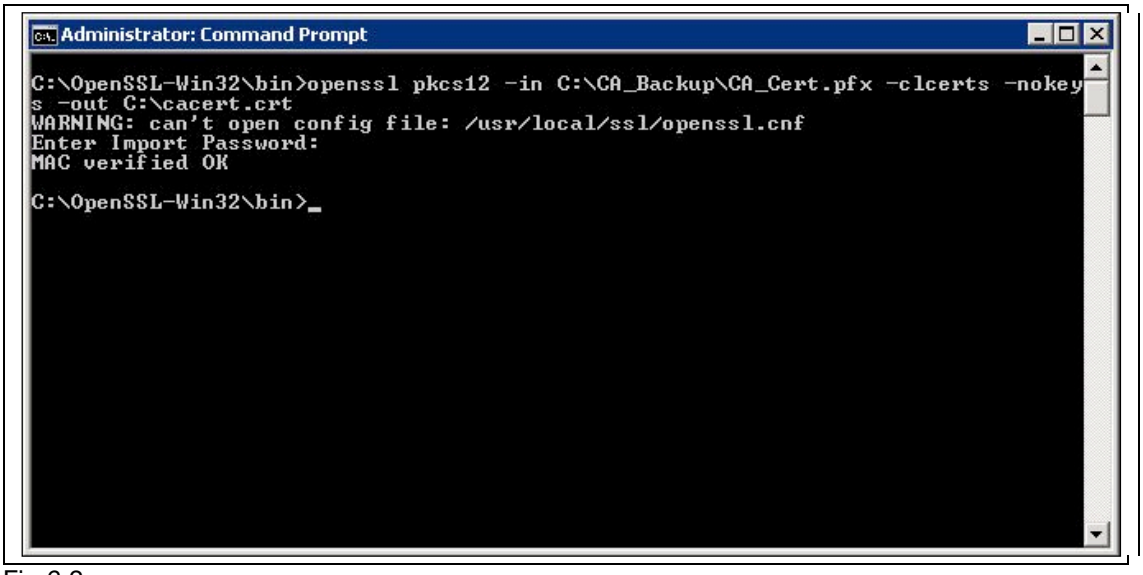


Fig 6.2

8. At this point, you will have two certificates located in the root of your C: directory:

   C:\privatekey.key
   C:\cacert.crt

Importing the Extracted Certificate and Private Key into FortiOS

1. Login to your FortiGate/FortiOS admin interface and go to **System** > **Certificates** > **Local Certificates**.

2. Click the "**Import**" link and select "**Certificate**" from the "**Type**" drop down list.

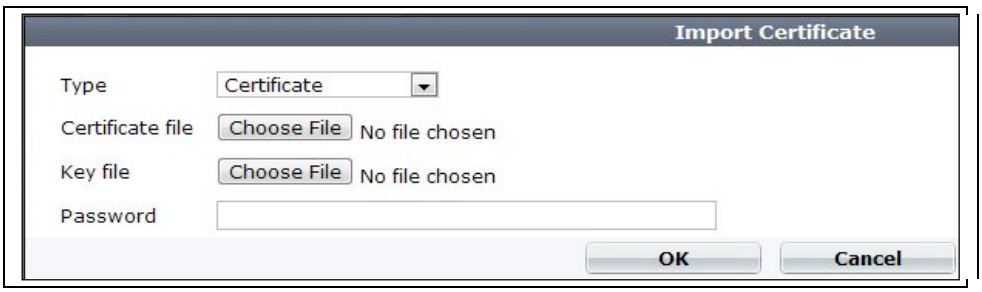


Fig 7.1

3. Click the "**Choose File**" button adjacent to "**Certificate file**". Select the cacert.crt file created in Fig 6.1.

4. Click the "**Choose File**" button adjacent to "**Key file**". Select the privatekey.key file created in Fig 6.2.

5. Enter the password that you created in Fig 6.1, then click "**OK**".

6. You should get the following message after clicking "OK" in the preceding step:

   Upload Certificate successfully. Return

7. Go to **System** > **Dashboard**. Scroll down to the "**CLI Console**" widget and click within the window.

8. At the command prompt, type the following commands:

```
config firewall ssl setting
      set caname <CAName>
      end
```

9. Substitute <CAName> with the name of the certificate that you imported into FortiOS. Examples of this can be found in Fig 2.2 under the "**Name**" column.

10. At this point, you have successfully imported your CA certificate and corresponding private key. You can now implement HTTPS proxy/inspection in your firewall policies.

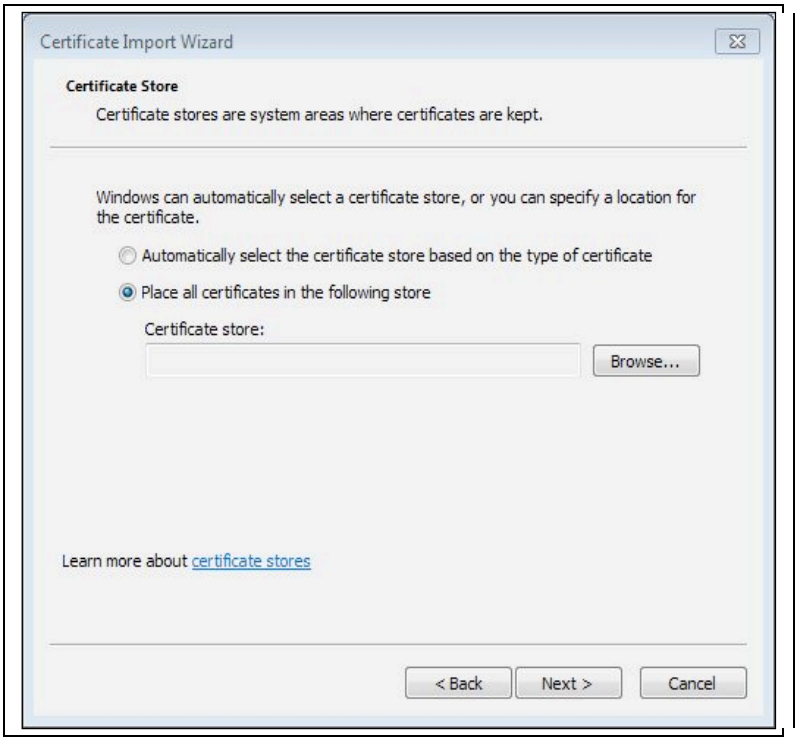
Importing the Extracted Certificate into the Certificate Store

Even though the CA/SSL certificate has been imported into FortiOS, HTTPS proxy/inspection will cease to function if the CA certificate is not installed in the certificate store of the client end point. I will now detail the import of the CA certificate into the Microsoft CAPI, the Mac OS X Keychain and the Java key store.

Microsoft CAPI Certificate Import

The CA certificate will need to be copied to the client end point file system.

1. Right-click the CA certificate and select "**Install Certificate**".
2. When the "**Certificate Install Wizard**" window appears, click "**Next**" to begin the import.
3. At the "**Certificate Store**" window, select the option, "**Place all certificates in the following store**" and click the "**Browse**" button.



8.1

4. In the “**Select Certificate Store**” window, select the option for “**Show physical stores**” then scroll up to “**Trusted Root Certification Authorities**” and select the sub-directory named, “**Local Computer**”.

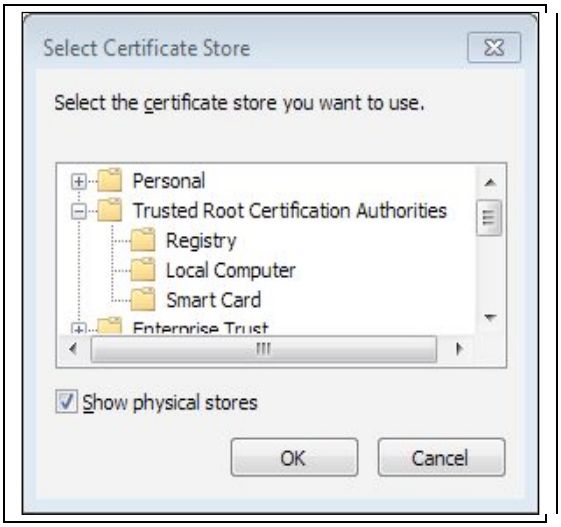


Fig 8.2

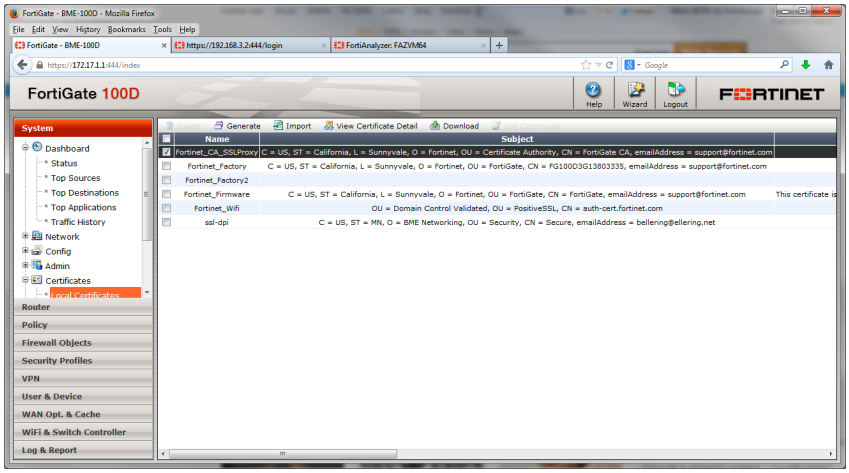
5. Click “OK” and then click “Next”. Once you click “Finish” on the final window, you will have successfully imported the CA certificate into the client end point certificate store.

Microsoft Group Policy Object Push

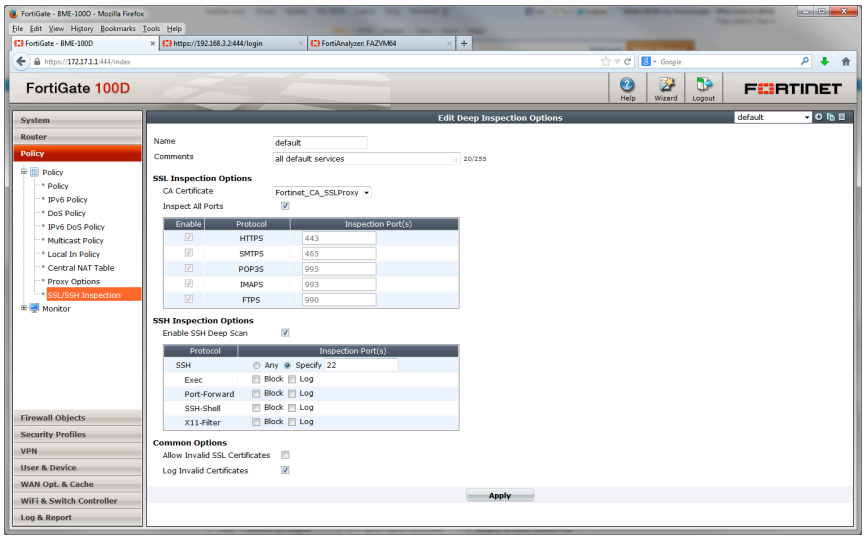
This section will illustrate how to push the FortiGate SSL Proxy CA (or your own, self-signed CA) to workstations using Group Policy Objects (GPO).

First, you will need to login to the FortiGate Administration GUI and go to **System** > **Certificates** > **Local Certificates**. In the screen shot below, you can see the selected “FortiGate SSL Proxy CA” certificate. This is the certificate that we will push out to all Windows workstations using GPO.

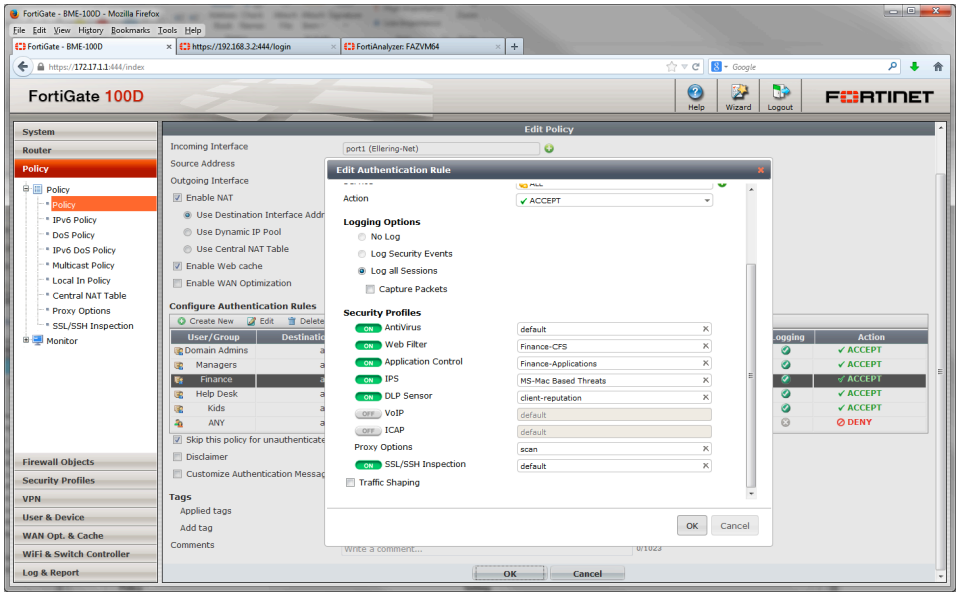
After selecting the aforementioned certificate, click the “**Download**” button at the top of the page. This will prompt you to save the Fortinet_CA_SSLProxy.cer file to your file system. We will use this file further down in this the guide.



Next, we need to configure the SSL Inspection properties. Via the FortiGate Administration GUI, go to **Policy** > **SSL/SSH Inspection**. Make any configuration changes needed, insuring that the FortiGate_CA_SSLProxy CA certificate is selected in the dropdown.



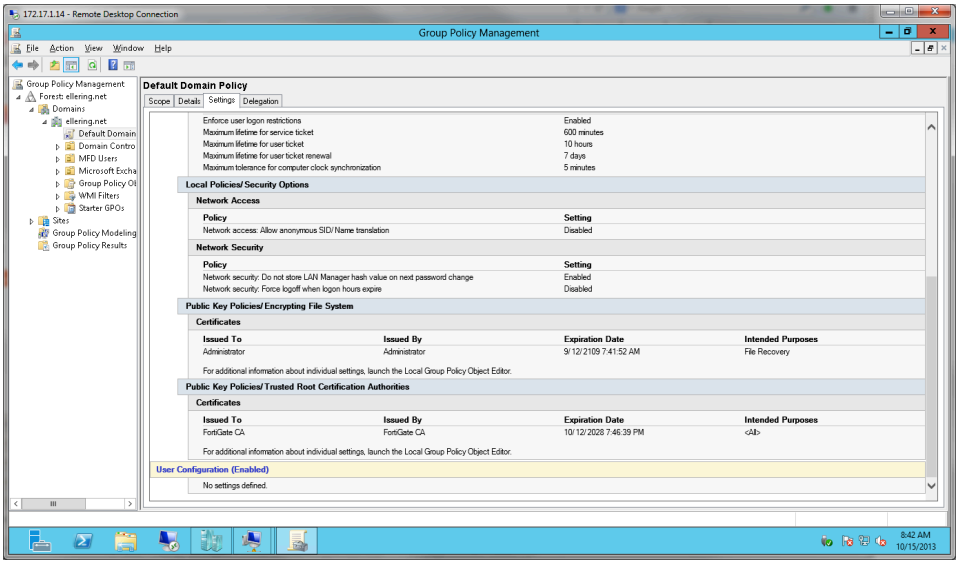
With this configuration completed, we will now enable the SSL/SSH Inspection in the policy where deep packet inspection is needed. Go to **Policy** > **Policy** and **create/edit** the policy where the inspection will be enforced. In the policy, simply scroll down to the section titled, “Proxy Options” and click the “On” button next to “SSL/SSH Inspection”. Once enabled, click the “OK” button to save the configuration.



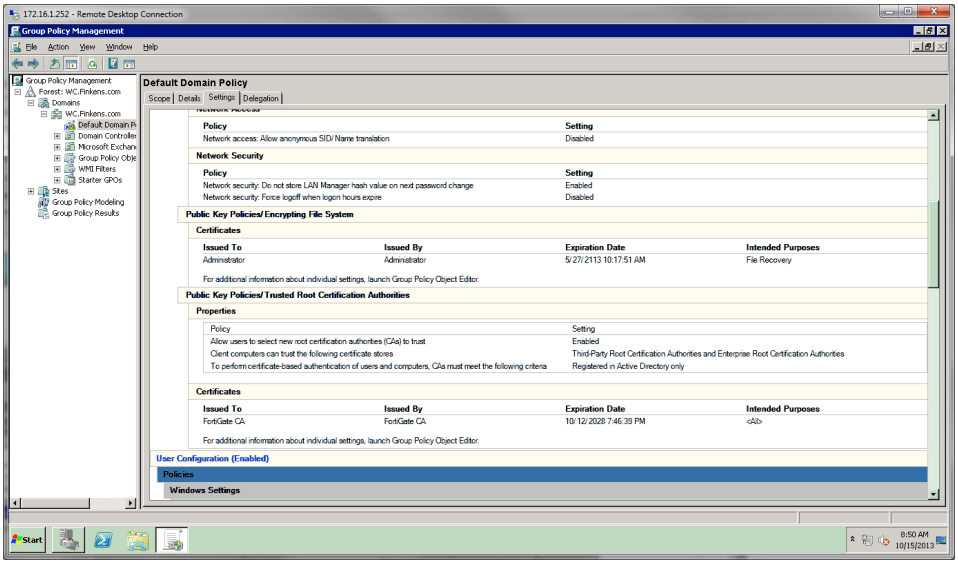
Now that the FortiGate configuration for SSL Inspection has been completed, we will now focus on deploying the FortiGate SSL Proxy CA certificate via Group Policy Objects. Below are screen shots of the GPO policies from Server 2012 and Server 2008 R2. These should be sufficient in getting the configuration created and pushed. Should you need further assistance with GPO for pushing certificates, please see the following link:

http://technet.microsoft.com/en-us/library/cc770315%28v=ws.10%29.aspx

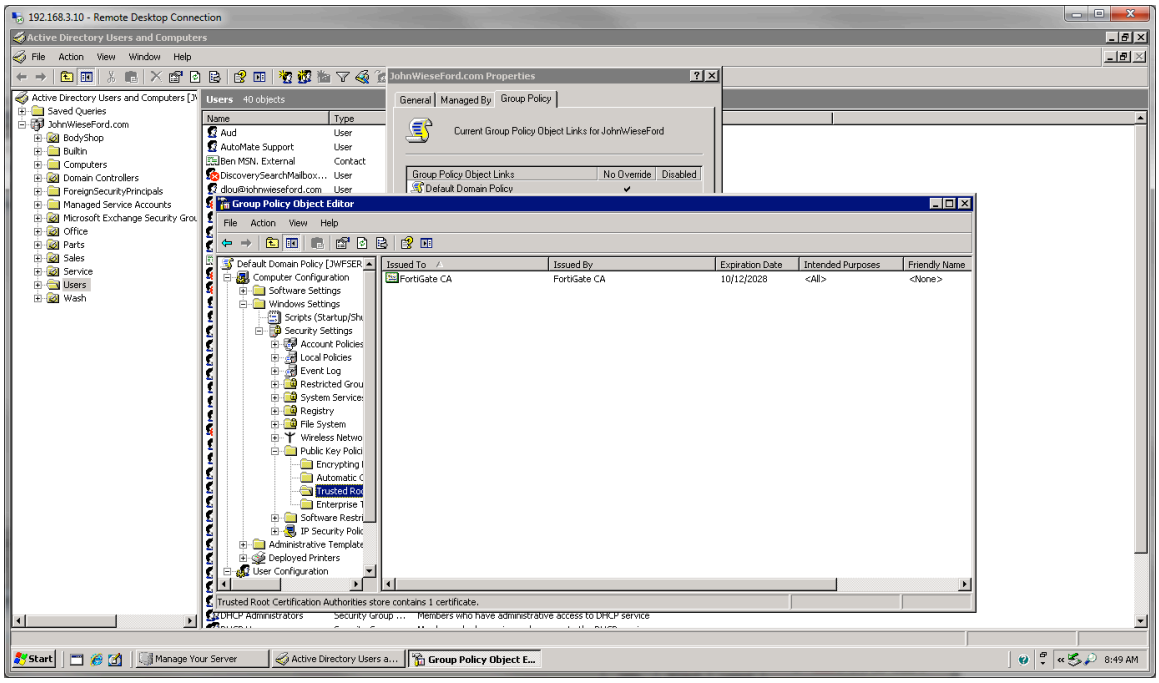
Group Policy Management – Windows Server 2012

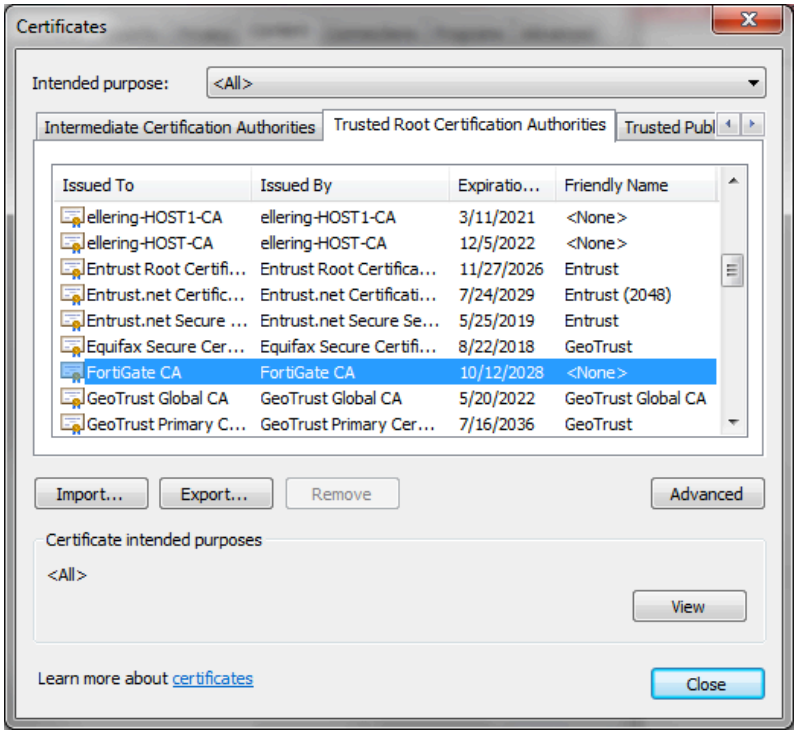


Group Policy Management – Windows Server 2008 R2



The following screen shots illustrate the FortiGate SSL Proxy CA residing in the Trusted Root Certification Authorities after being deployed via GPO.





Mac OS X Keychain Certificate Import

1. Open the Keychain Access utility from **Applications** > **Utilities**.
2. Choose **File** > **Import Items**.
3. Browse to the location of your P12 format certificate file, and click "**Open**".
4. You will be prompted to confirm the automatic trust the CA. To trust and install the CA certificate, click "**Always Trust**".

Java Keystore Certificate Import

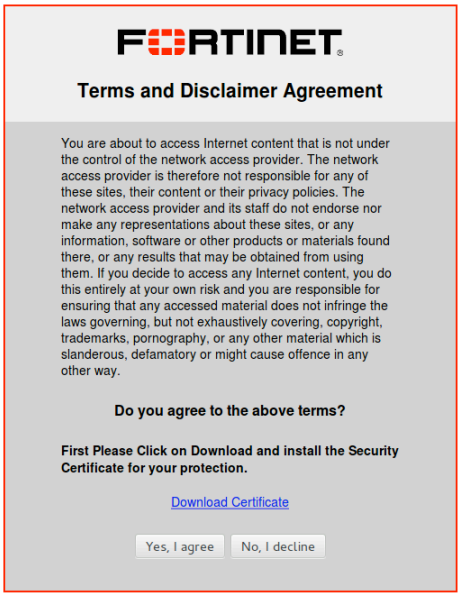
1. From the JRE/JDK bin directory, type the following command:

```
keytool -import -trustcacerts -alias CA -file <pathToCAcerFile> -
keystore <pathToKeystore> -keypass <keyPassword> -storepass
<storePassword>
```

Non-Domain Device/Guest Certificate Delivery Options

In most implementations of SSL inspection, mobile, non-domain and guest devices might also need the self-signed CA certificate in order for the inspection to work properly. Since GPO will not work for these devices, an alternative way to deliver the CA certificate is required.

Below is an example of a disclaimer page that contains the CA certificate in a download link:



This page can be created in the FortiOS Administration GUI by going to **System** > **Config** > **Replacement Messages** and modifying the Disclaimer Page under **Extended View** > **Authentication**. Below is the code used to create the disclaimer page shown above:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <style type="text/css">
      html,body{
        height:100%;
        padding:0;
        margin:0;
      }
      .oc{
        display:table;
        width:100%;
        height:100%;
      }
      .ic{
        display:table-cell;
        vertical-align:middle;
        height:100%;
      }
      form{
        display:block;
        background:#ccc;
        border:2px solid red;
        padding:0 0 25px 0;
        width:500px;
        font-family:helvetica,sans-serif;
        font-size:14px;
        margin:10px auto;
      }
      .fel,.fer,.fec{
        text-align:center;
        width:350px;
        margin:0 auto;
        padding:10px;
      }
      .fel{
        text-align:left;
      }
      .fer{
        text-align:right;
      }
      h1{
        font-weight:bold;
        font-size:21px;
        margin:0;
        padding:20px 10px;
        text-align:center;
      }
      p{
        margin:15px auto;
        width:75%;
        text-align:left;
      }
      ul{
        margin:15px auto;
        width:75%;
```

```
      }
      h2{
        margin:25px 10px;
        font-weight:bold;
        text-align:center;
      }
      label,h2{
        font-size:16px;
      }
      .logo{
        background:#eee center 25px url(%%IMAGE:logo_fw_auth%%) no-repeat;
        padding-top:80px;
      }
    </style>
    <body class="blocked">
      <div class="mobile">
        <div class="header">
          <body>
            <div class="oc">
              <div class="ic">
                <form action="/" method="post">
                  <input type="hidden" name="%%REDIRID%%" value= "%%PROTURI%%">
                  <input type="hidden" name="%%MAGICID%%" value="%%MAGICVAL%%">
                  <input type="hidden" name="%%ANSWERID%%" value="%%DECLINEVAL%%">
                  <h1 class="logo">
                    Terms and Disclaimer Agreement
                  </h1>
                  <p>
                           You are about to access Internet content that is not under
                    the control of the network access provider.  The network access
                    provider is therefore not responsible for any of these sites,
                    their content or their privacy policies. The network access
                    provider and its staff do not endorse nor make any representations
                    about these sites, or any information, software or other products
                    or materials found there, or any results that may be obtained from
                    using them. If you decide to access any Internet content, you do
                    this entirely at your own risk and you are responsible for
                    ensuring that any accessed material does not infringe the laws
                    governing, but not exhaustively covering, copyright, trademarks,
                    pornography, or any other material which is slanderous, defamatory
                    or might cause offence in any other way.
                  </p>
                  <h2>

                    Do you agree to the above terms?
                  </h2>
                  <h4>
                    <p style=:"text-align:center">
                      First Please Click on Download and install the Security
Certificate for your protection.
                    </p>
                  </h4>
                  <a href="data:application/x-x509-ca-
cert;base64,LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUQxekNDQXIrZ0F3SUJBZ0lCQURBTkJna3
Foa2lHOXcwQkFRVUZBRENCcFRFTE1Ba0dBMVVFQmhNQ1ZWTXgKRXpBUkJnTlZCQWdUQ2tOaGJHbG1iM0p1YVdF
eEVqQVFCZ05WQkFjVENWTjFibTU1ZG1Gc1pURVJNQThHQTFVRQpDaE1JUm05eWRHbHVaWFF4SGpBY0JnTlZCQX
NURlVObGNuUnBabWxqWVhSbElFRjFkR2h2Y21sMGVURVZNQk1HCkExVUVBeE1NUm05eWRHbEhZWFJsSUVOQk1T
TXdJUVlKS29aSWh2Y05BUWtCRmhSemRYQndiM0owUUdadmNuUnAKYm1WMExtTnZiVEFlRncwd09ERXdNVGd3TU
RRMk16bGFGdzB5T0RFd01UTXdNRFEyTXpsYU1JR2xNUXN3Q1FZRApWUVFHRXdKVlV6RVRNQkVHQTFVRUNCTUtR
MkZzYVdadmNtNXBZVEVTTUJBR0ExVUVCeE1KVTNWdWJubDJZV3hsCk1SRXdEd1lEVlFRS0V3aEdiM0owYVc1bG
RERWVNQndHQTFVRUN4TVZRMlZ5ZEdsbWFXTmhkR1VnUVhWMGFHOXkKYVhSNU1SVXdFd1lEVlFRREV3eEdiM0ow
YVVkaGRHVWdRMEV4SXpBaEJna3Foa2lHOXcwQkNRVdGSE4xY0hCdgpjblJBWm05eWRHbHVaWFF1WTI5dE1JSU
```

```
JJakFOQmdrcWhraUc5dzBCQVFFRkFBT0NBUThBTUlJQkNnS0NBUUVBCnR2ZURxNXZWaVNzUmdIUk9heWx0MHFN
ZHRlTGkxRC9MMEFXY3QrajVZK04rSHNrQnFzSzVlR0hyZ3l0VzZKcjMKZHRRLzUzL3VzVEkrOEhIcFBYajhnV3
VuZTZpdmpRY09BbUdzQi9nZndMUENhOTgra0xnbzl3cHUwTnhMVmJ5VQppNUY5T2pGdE1wRUdzWWxudTZqdHJz
SVI4RW9uQW5hVXRZS0NxUExOU1ZjL1U5N1pYOW03enlqTFlFR0VOdDJNCmVsbkFlVEROeTJWSGR4dmpDa0hCWl
l1SThseWd0UXNGdkFHZHZIc29JR0VLZ25MSGJ5Y0xDV1VrMWo5bVRrWUIKMFFGS1dkeTQ1anN2clVFbmFFdVdC
bElLTlpFZ3k4dUkxd1cvUnR2MUhIYm9mdVdyLzJnVElhZ2dQaklXc2hhawpzUEE1d1h0aDFONXBCTXJQT3hOb0
h3SURBUUFCb3hBd0RqQU1CZ05WSFJNRUJUQURBUUgvTUEwR0NTcUdTSWIzCkRRRUJCUVVBQTRJQkFRQnJBZkkr
VUx3ZzNNK2s0czNGQjYvLzZzUEc1VGNydlBkclE4Z0FyRWVZSkpDekhuVlkKdGtuSVBQeDFLNVYrUXVlQVhScE
xpdVdwaEZQNXc5T3hXdURxSHc4endiMjR3SmM3QkQ0Q2VGS1V5WWluYnBEaQpZZzAzNVNLWWw0VFNHTU9UaVlS
b1R4cWdrZnpjbVRGZnBmRDFwT0pRMDhLaCsxeWxlMzVXcUc5QWIxanJPMFkvCnZsdEdSZVpja3doOWU5NVNQek
5BNDN4R1pQU0lneFo4MDA3RVVxWUJla29TS0dBUVBxVGFsSEJrenBCMVVzM0YKNXlDWnp4QTRXWVQ5VUdWd1Bo
SVZnTWxadm01TkwyOS81ZEZndHM1MVUrUDRPWjBPcit4UWZXWUl4VHpDV3RBQwoxaWtaLzZIZUl2ZXQyN0g0Q1
BQMXJvbEJUWHc0ejZvbFAzMlQKLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo=">
                    <p style="text-align:center">
                      Download Certificate
                    </p>
                  </a>
                  <div class="fec">
                    <input type="submit" value= "Yes, I agree"
onclick="sb('%%AGREEVAL%%')">
                    <input type="submit" value= "No, I decline"
onclick="sb('%%DECLINEVAL%%')">
                  </div>
                  <script>
                    function sb(val) {
                      document.forms[0].%%ANSWERID%%.value = val;
                      document.forms[0].submit();
                    }
                  </script>
              </form>
              </div>
            </div>
          </body>
</html>
```

Implementing Deep Packet Inspection for SSL in FortiOS

This section will provide step-by-step details regarding the setup/implementation of HTTPS proxy/inspection in FortiOS.

As a general overview, FortiOS allows for the inspection of HTTPS sessions by instantiating two SSL tunnels: One between the client browser and FortiOS and one between FortiOS and the destination to which the client browser sent the request. This allows FortiOS to inspect the secured traffic using embedded UTM features. It is for this reason that the steps outlined above need to be completed before HTTPS proxy/inspection can occur.

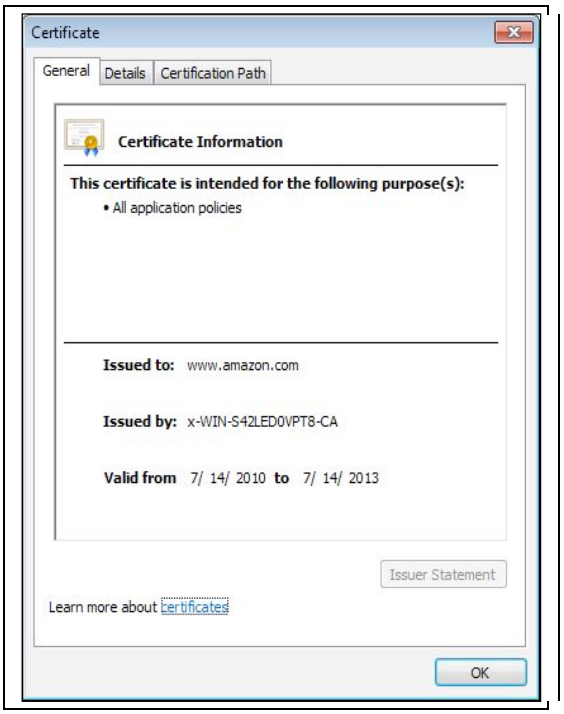
1. Login to FortiOS and go to **Firewall** > **Policy** > **SSL/SSH Inspection**.
2. For “CA Certificate”, select the appropriate certificate (e.g. Fortinet_CA_SSLProxy) from the drop down list.
3. Check the option to inspect all ports or simply use the “**Inspection Port(s)”** field to specify which ports you would like to inspect.
4. Once all settings have been configured, click “**Apply**”.

5. Go to **Firewall** > **Policy** and select or create a policy where SSL/SSH inspection should be used.

6. For the selected policy, select each security profile needed and enable the SSL/SSH Inspection option.

7. Click "**OK**" at the bottom of the page to save the policy settings.

8. Now you can test SSL inspection from a client browser to confirm that the configuration works. When you go to a page using HTTPS, the certificate will contain the site FQDN, but that it was issued by the CA that you imported into FortiOS. See the following screen shot for an example:



Exporting a Certificate from FortiOS

In the event that you need to export a certificate from FortiOS, there are two methods you can use to accomplish this.

GUI Export:

1. Login to FortiOS and go to **System** > **Certificates** > **Local Certificates**.

2. Select the certificate that you would like to export and click the "**Download**" link at the top of the page.

3. Save the certificate in a location of your choice.

CLI Export:

1. In the FortiOS command line interface, type the following command:

   ```
   fnsysctl cat /etc/cert/local/Fortinet_CA_SSLProxy.cer
   ```

   This command will list the certificate content in the console window similar to the following example:

   ```
   -----BEGIN CERTIFICATE-----
   MIID1zCCAr+gAwIBAgIBADANBgkqhkiG9w0BAQUFADCBpTELMAkGA1UEBhMCVVMx
   EzARBgNVBAgTCkNhbGlmb3JuaWExEjAQBgNVBAcTCVN1bm55dmFsZTERMA8GA1UE
   ChMIRm9ydGluZXQxHjAcBgNVBAsTFUNlcnRpZmljYXRlIEF1dGhvcml0eTEVMBMG
   A1UEAxMMRm9ydGlHYXRlIENBMSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRp
   bmV0LmNvbTAeFw0wODEwMTgwMDQ2MzlaFw0yODEwMTMwMDQ2MzlaMIGlMQswCQYD
   VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU3Vubnl2YWxl
   MREwDwYDVQQKEwhGb3J0aW5ldDEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9y
   aXR5MRUwEwYDVQQDEwxGb3J0aUdhdGUgQ0ExIzAhBgkqhkiG9w0BCQEWFHN1cHBv
   cnRAZm9ydGluZXQuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
   tveDq5vViSsRgHROaylt0qMdteLi1D/L0AWct+j5Y+N+HskBqsK5eGHrgytW6Jr3
   dtQ/53/usTI+8HHpPXj8gWune6ivjQcOAmGsB/gfwLPCa98+kLgo9wpu0NxLVbyU
   i5F9OjFtMpEGsYlnu6jtrsIR8EonAnaUtYKCqPLNSVc/U97ZX9m7zyjLYEGENt2M
   elnAeTDNy2VHdxvjCkHBZYuI8lygtQsFvAGdvHsoIGEKgnLHbycLCWUk1j9mTkYB
   0QFKWdy45jsvrUEnaEuWBlIKNZEgy8uI1wW/Rtv1HHbofuWr/2gTIaggPjIWshak
   sPA5wXth1N5pBMrPOxNoHwIDAQABoxAwDjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3
   DQEBBQUAA4IBAQBrAfI+ULwg3M+k4s3FB6//6sPG5TcrvPdrQ8gArEeYJJCzHnVY
   tknIPPx1K5V+QueAXRpLiuWphFP5w9OxWuDqHw8zwb24wJc7BD4CeFKUyYinbpDi
   Yg035SKYl4TSGMOTiYRoTxqgkfzcmTFfpfD1pOJQ08Kh+1yle35WqG9Ab1jrO0Y/
   vltGReZckwh9e95SPzNA43xGZPSIgxZ8007EUqYBekoSKGAQPqTalHBkzpB1Us3F
   5yCZzxA4WYT9UGVwPhIVgMlZvm5NL29/5dFgts51U+P4OZ0Or+xQfWYIxTzCWtAC
   1ikZ/6HeIvet27H4CPP1rolBTXw4z6olP32T
   -----END CERTIFICATE-----
   ```

2. Select and copy the certificate content including "`-----BEGIN CERTIFICATE-----`" and "`-----END CERTIFICATE-----`".

3. Open a text editor and paste the certificate content.

4. Save the file as CA.cer.

Managing Certificates in FortiClient

FortiClient is multi-functional end point security client that can utilize certificates for IPSec authentication to FortiOS. This section will focus on the import of a CA certificate as well as the generation of a CSR and import of an issued end-user certificate.

Importing a CA certificate into FortiClient:

1. Open the FortiClient GUI Console and go to **VPN** > **CA Certificates**.
2. Click the "**Import**" button at the bottom of the VPN: CA Certificates section.

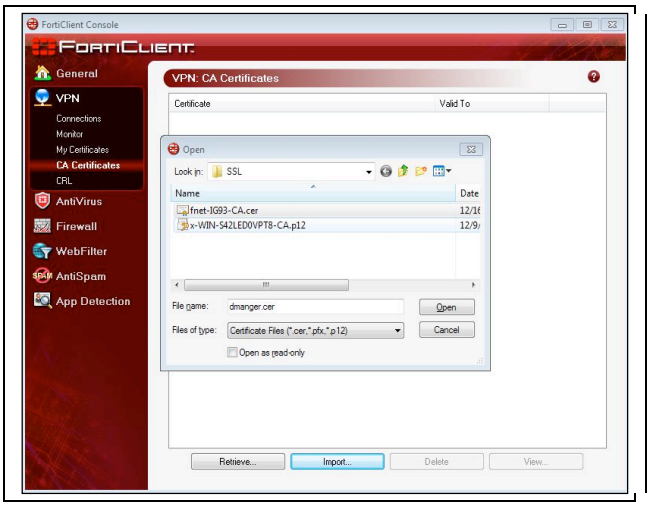


Fig 10.1

3. Select the CA certificate that was originally copied to the client end point in "Importing The Extracted Certificate Into The Certificate Store" section. You will get a message asking, "Do you want to import the relevant RA?" Click "**No**" unless your certificate authority requires a registration authority, as well.
4. You have now imported the CA certificate into FortiOS. Now you can proceed to end-user certificate creation.

Creating an end-user certificate in FortiClient

1. In the FortiClient GUI console, go to **VPN** > **My Certificates**.
2. Click the "**Generate**" button at the bottom of the VPN: My Certificates window. This will open the following window:

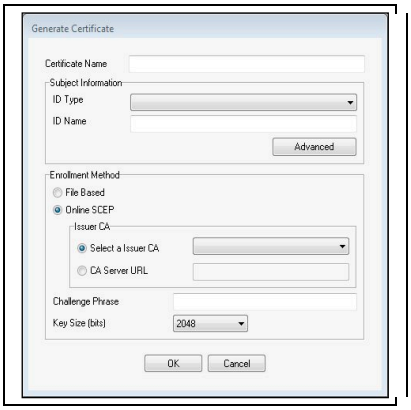


Fig 10.2

3. Under "**Generate Certificate**", fill out the following field/select the following options, then click "**OK**":

   Certificate Name: This will be the name displayed in the "Certificate" column under VPN: My Certificates. In the following example, I used, "Doug Manger, CISSP"

   Subject Information:
   ID Type: Select Email Address from the drop down list.
   Email Address: Enter the email address of the end-user who is requesting the certificate.
   Advanced: See the following sub-fields that will need to be completed.
   (Advanced)**Email**: This is the email address of the end-user who is requesting the certificate.
   (Advanced)**Department**: Enter the department with which the end-user is associated.
   (Advanced)**Company**: Enter the name of the company for which the end-user works.
   (Advanced)**City**: Enter the name of the city in which the end-user resides or works.
   (Advanced)**State/Province**: Enter the two-letter State/Province abbreviation where the end-user resides or works.
   (Advanced)**Country**: Select the country in which the end-user resides or works.

   Enrollment Method:
   File Based: Select this option if you do not plan to use or know if SCEP is supported in the environment.
   Online SCEP: Select this option if the organization supports certificate enrollment via SCEP. If supported, the end-user will need to speak with the certificate authority administrator to get the correct information on which option to select for **Issuer CA**.
   Challenge Phrase: This is the password that may be required by the certificate authority. Check with the certificate authority administrator to see if this is required.
   Key Size (bits): Select the certificate key size from the drop down list. Ask the certificate authority administrator which option to choose.

   See the following screen shots for an example of these values:

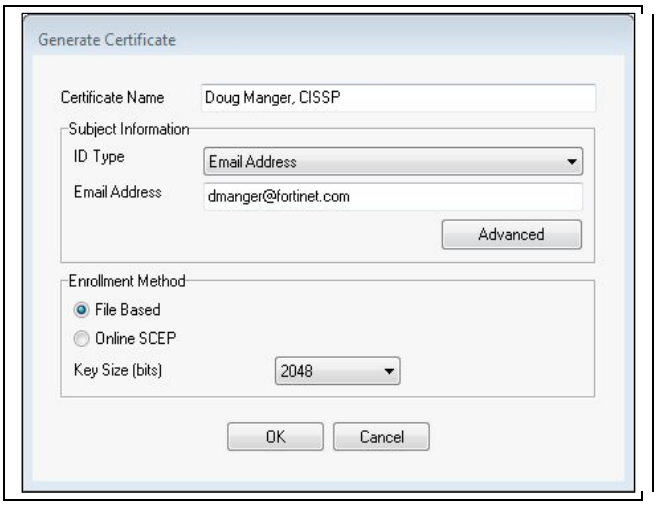


Fig 10.3

Fig 10.4

4. Now you will see the certificate request listed in the VPN: My Certificates list with a type of "**Request**". Select the request and then click the "**Export**" button at the bottom of the window.

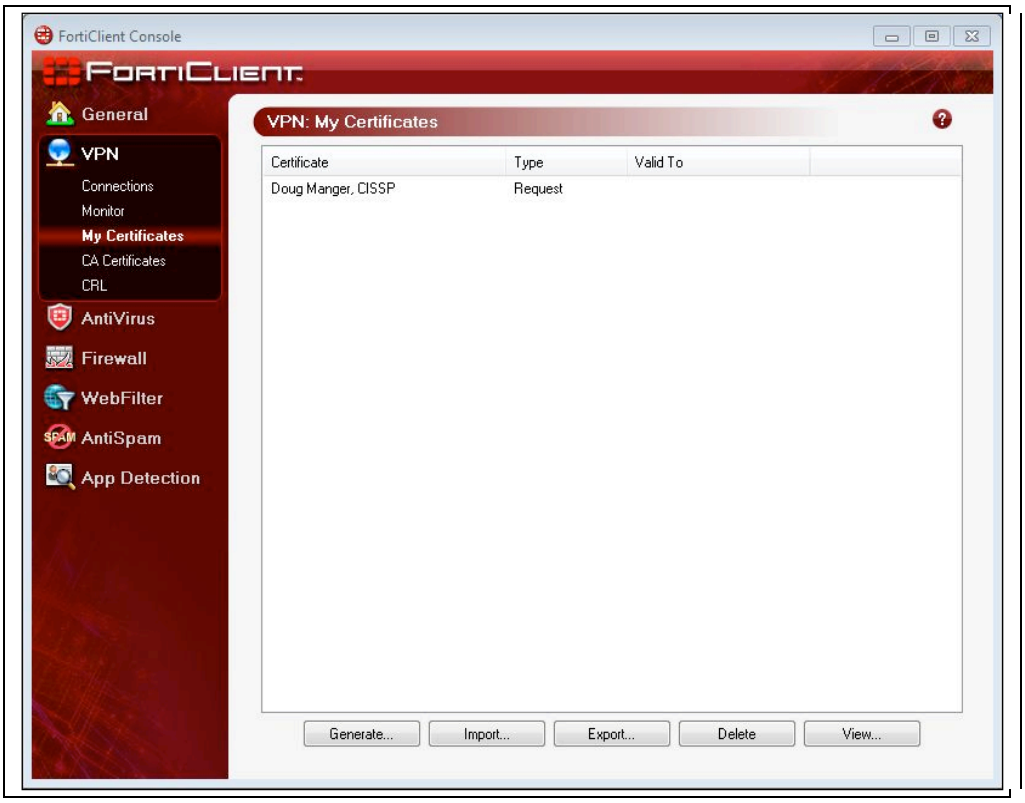


Fig 10.5

5. Choose a location where you would like the certificate signing request (CSR) saved and click "OK".

6. Send the CSR to the certificate authority administrator to process the request.

7. Once the certificate has been approved, copy the file to your file system.

8. In the VPN: My Certificates window, click the “**Import**” button and select the certificate that was created for the end-user, then click “**Open**”.

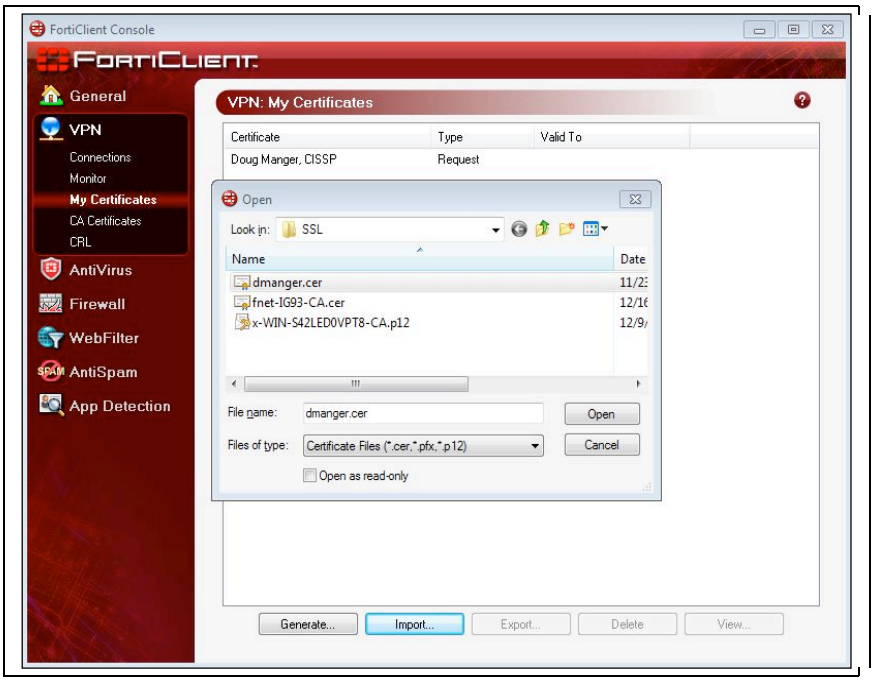


Fig 10.6

9. The end-user certificate will now show as a type of “**Certificate**” and provide a “**Valid To**” value.

Eliminating Certificate Warnings to Access FortiOS Admin Page

A common concern among customers is the fact that there is a certificate warning when an administrative user browses to the FortiOS login page. To eliminate these warnings, use the following steps below:

Import the self-signed FortiGate CA certificate into the end point certificate store:

1. Using the command/instructions found in the “Exporting A Certificate From FortiOS” section, export the self-signed FortiGate CA certificate and save it to a destination of your choice.

2. Using the steps from “Importing The Extracted Certificate Into The Certificate Store”, import the certificate that was exported in the previous step.

3. Browse to the hostname of your FortiGate device.

Leverage a CA-issued SSL certificate:

1. Login to FortiOS and go to **System** > **Certificates** > **Local Certificates**.

2. Follow the steps found in “Generating a CA-signed SSL Certificate” and “Importing a Certificate into FortiOS”.

3. Once the certificate is imported into FortiOS, go to **System** > **Network** > **DNS Server**.

4. Click "**Create New**" and enter the following information:

   DNS Zone: This is an arbitrary name that you will use for this DNS Zone.
   Domain Name: This is the root domain that you will use for the DNS Zone.
   TTL (seconds): Leave this at the default value unless you have a need to modify it.

5. Click "**OK**" and then click "**Create New**" under "**DNS Entries**".

6. Enter the following information for this DNS entry:

   Type: Select Address (A) from the drop down.
   Hostname: Enter the hostname of your FortiGate device. Example: fg1.fnet.local
   IP Address: Enter the IP address that will resolve from the hostname.
   TTL (seconds): Leave this at its default value unless there is a need to modify it.

7. Click "**OK**".

8. Connect to the FortiOS command line interface and enter the following commands:

   ```
   config system global
         set admin-server-cert wildcardssl
         end
   ```

   Note: The hostname of your FortiGate appliance will be the serial number. If you would like to change it to a more user-friendly name, add the following command to the this list:

   ```
   set hostname <newHostname>
   ```

9. Insure that the CA certificate that issued the SSL certificate is installed in the local certificate store of the end point. For details on installing the CA certificate into the local certificate store, go to "Importing The Extracted Certificate Into The Certificate Store".

10. Open a browser on the end point and browse to the FortiGate hostname created in step 6. The administration page will no longer show the certificate warning.

Certificate Authentication for IPSec and SSL VPNs

This section will cover the following topics:

- Client certificate creation using Microsoft Certificate Services
- Client Certificate creation using OpenSSL
- Setup Certificate Authentication for SSL VPN
- Setup Certificate Authentication for IPSec VPN

Client Certificate Creation Using Microsoft Certificate Services

1. Contact the Microsoft Certificate Services administrator to request a client certificate.

2. Once the certificate has been issued, follow the steps in the “Importing The Extracted Certificate Into The Certificate Store” section.

3. Proceed to the setup section below.

Client Certificate Creation Using OpenSSL

1. On the server where OpenSSL is hosted, open a command prompt to the OpenSSL bin directory and enter the following command:

   ```
   openssl  genrsa –des3 –out client.key 2048
   ```

   This command will prompt you to enter and validate a passphrase that will be used to protect the private key.

2. Next, type the following command to create the client certificate signing request:

   openssl req –new –key client.key –out client.csr

   This command will ask you to enter the following details:

   Country Name: This will be the two-letter abbreviation of the country where the CA will reside.
   State or Province Name: This is the full name of the state or province where the CA will reside.
   Organization Name: This is the name of the overall organization under which the CA will run.
   Organizational Unit: This is the name of the organizational unit under which the certificate will be issued. I have used “Sales” for my example since that is the organizational unit in which I reside.
   Common Name: This is the username of the end user to whom the certificate will be issued.
   Email Address: This should be the email address of the end user to whom the certificate will be issued.

3. The following command will complete the enrollment process and issue the client certificate:

   ```
   openssl x509 -req -days 365 -in client.csr -CA ca.crt -CAkey ca.key -
   set_serial 02 -out client.crt
   ```

4. Now you will need to enter a command that will combine the public and private keys for the client certificate into a pkcs12 format:

   ```
   openssl pkcs12 -export -in client.crt -inkey client.key -certfile
   cacert.crt -name "dmanger" -out client.p12
   ```

5. Copy the client.p12 file to the intended end point and follow the import instructions found in the “Importing The Extracted Certificate Into The Certificate Store” section.

6. Proceed to the next section for instructions pertaining to the setup of certificate authentication for SSL or IPSec VPN.

Setup Certificate Authentication for SSL VPN

1. Open a browser and go to your FortiGate administration page.

2. Go to **System** > **Certificates** > **CA Certificates**.

3. Import your CA certificate using the steps found in, “Importing The Extracted Certificate and Private Key Into FortiOS”.

4. Once the CA certificate has been successfully imported, go to the FortiGate CLI and enter the following commands:

```
config user peer
      edit <peerName>
            -- This is an arbitrary value of your choice.
            set ca <caname>
                  -- This is the CA certificate that you imported in step 3.
            set two-factor enable
            set password <password>
                  -- This is an arbitrary value of your choice.
```

Note: Use the following commands if they apply to your scenario:

```
set cn <cn>
```
-- This is the common name of the peer certificate. Use only if you wish to specify a single user certificate.

```
set ldap server <ldapServerName>
```
-- This is a LDAP server that you have setup under Users > Remote > LDAP – config user ldap.

```
set ldap-username <username>
```
-- This is an administrator account for your LDAP. You must use the full DN for this account (eg. cn=administrator, cn=users,dc=fnet,dc=local)

```
set ldap-password <password>
```
-- This is the password for the administrator account specified in the preceding command (set ldap-username).

```
set subject <certificateSubject>
```
-- If not set, this will allow any peer certificate subject. If you wish to isolate to just one user, enter any of the peer certificate name constraints.

5. Now you will create a user group for SSL VPN access:

```
config user group
      edit <groupName>  -- This is an arbitrary value of your choice.
            set sslvpn-access <portalName>
                  - Enter the name of the portal type for this group. Eg. full-access
            set member <memberName>
                  - This is the group(s) or user(s) who will be a part of the group.
            End
```

4. Configure your SSL VPN Policy:

```
config vpn ssl settings

      set sslvpn-enable enable
      set dns-server1 <dnsAddress>
      set reqclientcert enable
      set force-two-factor-auth enable
      set servercert <caIssuedSSLCert>
      set tunnel-ip-pools <ipPoolAlias>
      end
```

5. Configure your firewall rules:

```
config firewall policy
      edit <policyNumber>
            set srcintf <sourceInterface>
            set dstintf <destinationInterface>
            set srcaddr <sourceAddress>
            set dstaddr <destinationAddress>
            set action sslvpn
            set sslvpn-ccert enable
            end
      config identity-based-policy
            edit <policyNumber>
                  set schedule <schedule>
                  set logtraffic <enableOrDisable>
                  set groups <peerGroupName>
                  set service <serviceType(s)>
                  end
```

6. Open a browser and go to https://<FGAddress>:10443/remote/login to test client certificate authentication. If all settings have been configured correctly, the end user should be prompted for his/her certificate and, upon confirmation of said certificate, will then have full access to the profile assigned to his/her group. If the user gets a certificate prompt and a subsequent username and password field page, there is a problem with either the certificate chain or the validation of the user.

   To troubleshoot issues related to certificate authentication, use the following commands:

```
diagnose debug app fnbamd 7
diagnose debug enable
```

   Read the console output to see what errors occur. Send any output to TAC for troubleshooting assistance.

Setup Certificate Authentication for IPSec VPN

1. In the FortiGate cli, begin the certificate-based IPSec configuration with the following command:

```
config vpn ipsec phase1-interface
      edit <phase1Name>
            set type dynamic
            set interface <interface>
```

```
            set proposal 3des-sha1 aes128-sha1
            set authmethod rsa-signature
            set peertype peergrp
            set rsa-certificate <caCert>
            set peergrp <peerGroupAlias>
            end
```

This will set up your phase 1, interface mode, auto key (IKE).

2. Next you will setup your phase 2 configuration:

```
config vpn ipsec phase2-interface
      edit <phase2Name>
            set keepalive enable
            set phase1name <phase1Name>
            set proposal <proposal1> <proposal2>
            - be sure to mirror the proposals you set in phase 1
            set dhcp-ipsec enable
            end
```

3. Configure your IPSec firewall policy.

   The following is an example of a firewall policy that leverages certificate authentication:

```
edit 14
      set srcintf "wlan"
      set dstintf "WLANCert"
      set srcaddr "all"
      set dstaddr "IPSec_DHCP"
      set action accept
      set schedule "always"
      set service "ANY"
      set logtraffic enable
      set nat enable

edit 15
      set srcintf "WLANCert"
      set dstintf "wlan"
      set srcaddr "IPSec_DHCP"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set logtraffic enable
      set nat enable
```

4. On the user end point, open the FortiClient console and go to VPN.

5. Right-click in the VPN: Connections window and select “**Add…**”

6. Modify the following values:

   Connection Name: Arbitrary alias for the VPN connection.
   VPN Type: Select the option for “Manual IPSec”
   Remote Gateway: IP/Hostname of your FortiGate VPN interface.
   Remote Network: IP Range of the IPSec address pool. This will be provided by the FortiGate admin.
   Authentication Method: Select either “X509 Certificate” or “SmartCard X509 Certificate”.
   (SmartCard) X509 Certificate: Select your certificate from the drop down list.

7. Click “OK”, right-click the new VPN entry and select “Test”. This will test the connection to FortiGate. If successful, right-click the entry and select “Connect”. This will connect the end user by way of his/her client certificate.